Saksframlegg

Saksgang:

Styre	Møtedato
Styret Sykehuspartner HF	22. mai 2024

SAK NR 035-2024

TRUSSELVURDERING FOR SPESIALISTHELSETJENESTEN 2024

Forslag til vedtak:

Styret tar rapporten til etterretning

Skøyen, 15. mai 2024

Hanne Tangen Nilsen
administrerende direktør

Vedlegg:
Trusselvurdering 2024 – det digitale trusselbildet mot spesialisthelsetjenesten

1. Hva saken gjelder

Trusselvurderingen for spesialisthelsetjenesten utarbeides på bakgrunn av de åpne trusselvurderingene fra E-tjenesten, Politiets sikkerhetstjeneste (PST) og Nasjonal sikkerhetsmyndighet (NSM), også omtalt som EOS-tjenestene. Årets rapport er, som i 2023, utarbeidet i samarbeid mellom de fire regionale IKT-foretakene og Helse CERT (Norsk helsenett).

Formålet med rapporten er å sikre en omforent situasjonsforståelse blant ledere og medarbeidere i spesialisthelsetjenesten slik at vi bedre evner å vurdere risiko vi står ovenfor. Trusselvurderingen skal gi innsikt i hvordan man kan forstå hva som truer spesialisthelsetjenestens verdier og hvilken risiko dette utgjør. Trusselaktørene og deres angrepsmetoder må løpende vurderes og overvåkes, samtidig som det må skapes forståelse i organisasjonen for hvordan våre sårbarheter kan utnyttes av disse. Systematisk og god håndtering av sårbarheter vil være det viktigste virkemiddelet for å redusere risiko.

Spesialisthelsetjenesten er en grunnleggende tjeneste i samfunnet og har en viktig beredskapsfunksjon for ivaretakelse av liv og helse. Dette gjør spesialisthelsetjenesten trusselutsatt på lik linje med andre deler av totalforsvaret og kritisk infrastruktur.

2. Hovedpunkter

Et vellykket cyberangrep mot spesialisthelsetjenesten kan medføre store konsekvenser for spesialisthelsetjenestens evne til å utføre sine primæroppgaver. Dagens trusselbilde er komplisert og i konstant endring som følge av trusselaktørenes økte tilpasningsevne og utvikling av verktøy og metoder. Statistikken globalt viser en økning av angrep mot helsesektoren – helsesektoren er den 3. mest angrepsutsatte sektoren.

Destruktive angrep i form av digital utpressing fra organiserte kriminelle aktører utgjør den største trusselen. Slike angrep benytter sårbarheter i programvare gjennom ransomware/løsepengevirus som gjør data og løsninger kryptert og utilgjengelig og låses opp mot betaling. Veien ut er betaling eller gjenoppretting fra sikkerhetskopier.

Cyberoperasjoner og rekruttering av innsidere vil være blant de mest sentrale metodene for statlige aktører i 2024, og det forventes at Russland og Kina vil være spesielt aktive i sine forsøk på å rekruttere kilder og innsidere.

Aktørutvikling

Global statistikk viser at angrep mot helsesektoren har økt, sett opp mot fjoråret. Organiserte kriminelle aktører står bak de fleste angrep. De er opportunistiske og økonomisk motiverte med en økende grad av kartlegging og målrettet aktivitet mot de med betalingsevne og vilje. De kriminelle økosystemene er også påvirket av den geopolitiske situasjonen, et eksempel er at russiske grupperinger av ulike trusselaktører opplever forstyrrelser og endringer. Gjennom det siste året har det vært en 20% økning i omsetning knyttet til kompromitterte tilganger som kjøpes og selges i all hovedsak mellom organiserte kriminelle, men også statlige aktører. Dette er en trend man forventer vil fortsette og aktørene som spesialiserer seg på salg av tilganger knytter tettere bånd til aktørene som utvikler verktøy.

I de åpne trusselvurderingene fra EOS tjenestene beskrives Russland, som den største etteretningstrusselen mot Norge, og Kina som en økende trussel. Den økte aktiviteten fra disse aktørene ses i all hovedsak i cyberdomenet. Russland har mistet diplomatisk fotfeste i vesten, og bare i Norge har 15 russiske diplomater blitt utvist siden krigen i Ukraina startet, noe som medfører

at de må finne alternative informasjonskilder. For spesialisthelsetjenesten betyr det blant annet økt innsiderisiko.

Statlige aktører fokuserer på spionasje og informasjonslekkasje og i liten grad destruktive cyberoperasjoner. Unntaket er Nord-Korea som benytter både offentlig kjente skadevarer og egenutviklede skadevarer i cyberangrep. Nord-Korea utnytter sårbarheter i internetteksponerte tjenester og skytjenester, og det har blitt observert kampanjer hvor målsetningen er å få tilgang til påloggingsopplysninger for å benytte disse i senere angrep.

Forskningsdata, informasjon om beredskap, og sensitiv informasjon som helse- og personopplysninger er noen av verdiene som statlige aktører ønsker tilgang til. Globalt er det medisinsk forskning et område som spesielt statlige aktører er opptatt av. Spesialisthelsetjenesten har tette forbindelser med ulike forskningsinstitusjoner, og forskning er en viktig og integrert del av helsesektoren. I økende grad benytter aktørene innsidere, tredjeparter og underleverandører for å få tilgang til informasjon. Dette krever økt oppmerksomhet på innsiderisiko, innsikt og kontroll på leverandørkjeder samt bedre forståelse for verdiene spesialisthelsetjenesten besitter.

De åpne trusselvurderingene fra PST, NSM og E-tjenesten viser alle et skjerpet trusselbilde knyttet til leverandørkjeder og statlige aktører. Det er krevende å gjennomføre anskaffelser ved å balansere nytteverdi av utstyr opp mot sårbarheter og avhengigheter i leverandørkjedene. Leverandørkjedene er ofte lange og med forgreininger til leverandører fra høyrisikoland. I en sektor med krevende økonomi er det i anskaffelser utfordrende å ivareta krav til sikkerhet når disse leverandørenes tilbud ivaretar alle funksjonelle krav til en lav pris. Dette gjelder spesielt løsninger som ikke omfattes av sikkerhetsloven.

Hacktivisters evne til å utgjøre en trussel varierer kraftig. Enkelte grupper er ikke i stand til å utføre mer enn forstyrrende DDoS-angrep, mens andre har kapasiteten til å gjennomføre større koordinerte operasjoner og kompromittere utvalgte mål. En økning i evne hos enkelte grupperinger har man likevel sett det siste året, der flere store vellykkede angrep har blitt gjennomført.

Teknologiutvikling gir nye angrepsflater

Bruk av skytjenester øker i omfang, noe som øker kompleksiteten og angrepsflaten. Skytjenestene er gjerne tett integrert med interne IKT-systemer, der en hybrid tilnærming kan skape en utilsiktet ekstern eksponering av interne tjenester. *Retail & Hospitality Information Security and Analysis Center* (RH-ISAC) viser til eksempler med feilkonfigurering av servere i skymiljø som eksponeres mot Internett, og ikke bare interne soner, som dermed kan kompromitteres og gir mulighet for videre utnyttelse innover i nettverket. Samtidig gir skytjenester store muligheter for realisering av gevinster fra teknologiutvikling og digitalisering, samt at det kan bidra til bedre sikkerhet.

Kunstig intelligens er systemer som utfører handlinger, fysisk eller digitalt, basert på tolkning og behandling av strukturerte eller ustrukturerte data for å oppnå et spesifikt mål. Virksomheter må ta i bruk kunstig intelligens på en trygg og ansvarlig måte. Dette skaper ujevne odds ved at trusselaktørene kan ta i bruk teknologien raskere uten tanke på trygge rammer og reguleringer. Flere rapporter viser til en dramatisk økning av falske videoer benyttet i bedragerier. I Hong Kong ble en regnskapsmedarbeider lurt til å overføre 200 millioner HK dollar etter en 45 minutter lang videokonferanse. I ettertid avdekket etterforskningen at regnskapsmedarbeideren var eneste mennesket i samtalen, de andre deltakerne var KI genererte avatarer.

3. Administrerende direktørs anbefaling

For å motstå avanserte cyberangrep kreves det en helhetlig tilnærming til sikkerhetsarbeidet hvor en må ha grunnleggende og gode sikkerhetsbarrierer som stopper både opportunistiske angrepsforsøk og angrep fra avanserte statlige aktører. Spesialisthelsetjenesten må derfor ha velutviklede metoder for å avdekke uønsket aktivitet, for å håndtere denne aktiviteten og for å igangsette nødvendige risikoreduserende tiltak.

Rapporten vil bli benyttet ved utarbeidelse av bevisstgjørings- og opplæringstiltak i Sykehuspartner HF, som del av autorisasjonssamtaler knyttet til Sikkerhetsloven, og som grunnlag for vurderinger i arbeid med risiko- og sårbarhetsvurderinger. Den vil bli presentert for alle ledergrupper på nivå 2 og relevante målgrupper i Sykehuspartner samt styret i Helse Sør-Øst.

Administrerende direktør anbefaler at styret tar rapporten til etterretning.